LARA LICENSING AND REGULATORY AFFAIRS	**Effective Date:**	06-21-2019
	Policy #:	G-42
	Supersedes:	09-12-2011
Subject: **Criminal History Record Information Security**	**Page:**	1 of 13

PURPOSE

LARA is considered a Noncriminal Justice Agency (NCJA) and is an Authorized Recipient (AR), wherein certain Authorized Personnel are able to request and receive fingerprint-based Criminal History Record Information (CHRI) checks. Authorization for ARs to receive CHRI is for the purpose of employment, licensing, or volunteer determinations. Therefore, LARA is to ensure compliance with applicable state and federal laws, applicable rules and regulations, the most current version of the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy, in addition to LARA policies, procedures, and processes. This Information Security Policy provides the appropriate access, maintenance, security, confidentiality, dissemination, integrity, and audit requirements of CHRI in all its forms, whether at rest or in transit.

The most stringent requirement shall prevail if conflict(s) is/are found between agency policies, state or federal laws, with the most current version of the FBI CJIS Security Policy, and corresponding rules, or regulations.

As used in this policy:
(a) **Authorized Recipients** - (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.
(b) **Authorized User/Personnel** - An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based background check, where required, and have been granted access to CJI data, wherein access is only for the purpose of evaluating an individual's qualifications for employment or assignment.

USER AGREEMENT

LARA shall complete and maintain a Noncriminal Justice Agency User Agreement for Release of Criminal History Record Information (RI-087) provided by the Michigan State Police (MSP). Agreements are in place to provide for data ownership, individual roles, responsibilities, etc. When changes in contact information (address, e-mail address, contact name, etc.) occur, the LARA shall complete and return a new user agreement. The most current copy of this user agreement will be maintained on file at the agency indefinitely.

LOCAL AGENCY SECURITY OFFICER (LASO)

The LARA Bureau Director and LARA Privacy Officer will designate a LASO by means of completing and returning to the MSP, Security & Access Section (SAS), a Noncriminal Justice Agency Local Agency Security Officer Appointment (CJIS-015). An individual designated as LASO is:

- An "authorized user/personnel."
- An individual that has completed a fingerprint-based background check, where required, and found appropriate to have access to CHRI.
- If a school, the LASO is an employee directly involved in evaluating an individual's qualifications for employment or assignment.

A LASO is responsible for the following:

- Identifying who is using or accessing CHRI and/or systems with access to CHRI.
- Identifying and documenting any equipment connected to the state system.
- Ensuring personnel security screening procedures are being followed as stated in this policy.
- Confirming the approved and appropriate security measures are in place and working as expected.
- Supporting policy compliance and ensuring the MSP Information Security Officer (ISO) is promptly informed of security incidents.

When changes in the LASO appointment occur, LARA shall complete and return a new LASO appointment form. The most current copy of the LASO appointment form will be kept on file indefinitely by the agency (CJIS-015).

All MSP fingerprint account changes are to be made by the LASO.

PERSONNEL SECURITY

ALL PERSONNEL

All personnel requiring access to CHRI must first be deemed "Authorized Personnel." The LASO or authorized designee will review and determine if access is appropriate. Access is denied if:

a. The law prohibits the individual from working in or with LARA.
b. The individual has ever had a felony, of any kind, no matter when it occurred.

If a record of any other kind is found, the LASO or authorized designee will review if access is appropriate. Persons believed to be a fugitive, or having an arrest history without conviction must be reviewed to determine if access to CHRI is appropriate. The LASO or authorized designee may ask for a review by the CJIS Systems Officer (CSO) of the MSP in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

Access will be granted upon determination by the LASO or authorized designee, so long as providing such access would not be detrimental to the agency or the individual for which the record pertains.

Persons with access to CHRI and are subsequently arrested and/or convicted of a crime will:

a. Have their access to CHRI suspended until the outcome of an arrest is determined and reviewed by the LASO or authorized designee in order to determine if continued access is appropriate.
b. Have their access suspended indefinitely if a conviction results in a felony of any kind.
c. Have their access denied by the LASO or authorized designee where she/he determines that access to CHRI by the person would not be in the public's best interest.

Whenever possible, access to CHRI by support personnel, contractors, and custodial workers will be denied. If a need should arise for such individuals to be in an area(s) where CHRI is maintained or processed (at rest or in transit); persons will be escorted by or under the supervision of authorized personnel at all times while in these area(s).

Contracted Information Technology (IT) contractors or vendors will be physically or virtually escorted by authorized personnel anytime said individuals have access to facilities, areas, rooms, or an agency's CHRI information system.

Virtual escorting of privileged functions is permitted only when all the following conditions are met:

1. The session shall be monitored at all times by an authorized escort.
2. The escort shall be familiar with the system/area in which the work is being performed.
3. The escort shall have the ability to end the session at any time.
4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced.
6. Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

NCJAs that do not have passed and federally approved legislation authorizing or requiring the civil fingerprint-based background checks are exempt from this requirement until such a time as appropriate legislation has been written into law.

PERSONNEL SCREENING FOR CONTRACTORS AND VENDORS

In addition to the screening requirements provided in the immediate preceding areas, contractors and vendors (persons with access to agency system hardware or software) shall meet the following requirements:

a. If a record of any kind is found, delay access until the LASO or authorized designee can review the record and determine such access to CHRI is appropriate.
b. If a felony record of any kind is found, access will be denied.
c. If a confirmed outstanding arrest warrant is found, access will be denied.

LARA will retain and keep current a list of personnel who have been given authorized access to CHRI, and make this list available to the MSP upon request.

NCJAs that do not have passed and federally approved legislation authorizing or requiring the civil fingerprint-based background checks are exempt from this requirement until such a time as appropriate legislation has been written into law.

PERSONNEL TERMINATION

The LASO or authorized designee shall terminate access to CHRI immediately, which is within 24 hours of a notification that an individual's termination of employment has occurred. These procedures are set forth by LARA here: http://www.michigan.gov/lara/0,4601,7-154-10573_35828_59075-296503--,00.html

DTMB Common Control (Applies to the DTMB Technical LASO):

DTMB Administrative Policy 100.25 Employee Departures

This policy outlines the requirements for ensuring all state technology devices and accesses granted to employees (i.e., state employee, temporary employee, and student/intern) are returned and accesses removed promptly upon employee departure. Employee departure includes:

- Resignation
- Retirement
- Termination
- Transfer to another work unit or department
- Reassignment within the department
- Layoff
- Leave of Absence, subject to needs of the work area

These devices include, but are not limited to:
- Building access cards and/or door, cabinet, cubicle keys
- Desktop and supporting equipment and cords
- Laptop and supporting equipment and cords
- Wireless communication devices (cell phones, Smartphones, etc.) and chargers, clips, etc.
- Wireless Internet/remote access devices (Secure ID tokens/drives/cards)
- Phone calling cards
- Procurement cards
- Equipment (i.e., radios, tools, manuals, calculators, etc.)

MCSC C-636 Employee/Contractor Departure Checklist (Applies to all DTMB Contractors):
It is the responsibility of the manager to conduct an exit interview with the departing employee using the Employee Departure Checklist, C-636. This form is for all IT Assets, IT Security, Facility Security, Passwords, Human Resources and Other such as phone credit cards, procurement cards, state vehicle keys which an employee may have. Form is for leaving state government, transferring to another state department or transferring within DTMB. To remove security access the Client Service Center (CSC) is contacted and a DTMB-0161 Network User ID Request is completed.

MCSC CS-301 Employee Departure Report (Supervisors are required to submit this on the employee's last day of work)

According to DTMB 1340.00.140.01 Personnel Security Standard, Information System Owners must ensure that the agency implements and documents the disabling of information system access within 24 hours of employee termination.

LARA Common Control:
LARA Supervisors complete an online departure form that notifies the proper individuals to terminate network access and remove users from LARA information systems. LARA Supervisors complete an exit interview checklist that ensures employee identification cards, building access cards, procurement cards, building keys, and equipment are collected and handled in accordance with Department policy.

DTMB Common Control:
The Michigan Civil Service Commission provides policy for state employee position categorization, personnel screen, personnel termination and transfer.
Upon separation or transfer, a Network User ID Request DTMB-0161 form and an Employee/Contractor
Departure Checklist form MCSC C-636 is required to be completed.

LARA Common Control:
LARA Supervisors review and confirm ongoing need for the employee to have logical and physical access to the information system and building. They also complete an online departure form that notifies the proper individuals to terminate network access and remove users from LARA information systems. LARA Supervisors complete an exit interview checklist that ensures employee identification cards, building access cards, procurement cards, building keys, and equipment are collected and handled in accordance with Department policy

PERSONNEL TRANSFER
Individuals with access to CHRI, and where the individual has been reassigned or transferred, shall have his or her access reviewed by the LASO or authorized designee to ensure access is still appropriate. If access is determined to be suspended, the individual shall be restricted from access to CHRI within the immediate 24 hours of transfer or reassignment and the following steps shall be taken by LARA immediately:

a. This is addressed in the Personnel Termination Section.

SANCTIONS
Persons found noncompliant with state or federal laws, current FBI CJIS Security Policy, rules or regulations, including LARA Information Security Policy, will be formally disciplined. Discipline can be, but not limited to, counseling, the reassignment of CHRI responsibilities, dismissal, or prosecution. Discipline will be based on the severity of the infraction and at the discretion of LARA.

MEDIA PROTECTION

CHRI media is to be protected and secured at all times. The following is established and is to be implemented to ensure the appropriate security, handling, transporting, and storing of CHRI media in all its forms.

MEDIA STORAGE & ACCESS
Digital and physical CHRI media shall be securely stored within physically secured locations or controlled areas, and within the agency's facility unless otherwise permitted. Access to such media is restricted to authorized personnel only and secured at all times when not in use or under the supervision of an authorized individual.

Physical CHRI media:

a. Is to be stored within individual records when feasible or by itself when necessary.

b. Is to be maintained within a lockable filling cabinet, drawer, closet, office, safe, or vault, etc

Digital CHRI media:

a. Is to be secured through encryption as specified in the most current FBI CJIS Security Policy.
b. Unless encrypted, digital storage media devices (such as discs, CDs, SDs, thumb drives, DVDs, etc.) are to be maintained within a lockable filling cabinet, drawer, closet, office, safe, or vault, etc.

MEDIA TRANSPORT (DIGITAL AND/OR PHYSICAL)
Should the need arise to move CHRI media outside of the secured location or controlled area, the Department of Licensing and Regulatory Affairs shall establish and implement appropriate security controls to prevent compromise of the data while transporting. The transport of CHRI media will be conducted by authorized personnel.
CHRI media includes:

- Physical CHRI media such as paper/hard copies.
- Digital CHRI media such as laptops and computer hard drives and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card(s).

The record is to be transferred to and from the designated room in a sealed envelope. This will not be necessary when CHRISS is available as records can be accessed through the CHRISS system. Each work area will be able to directly access the record through the CHRISS system and the passing of the record will no longer be required.

DIGITAL MEDIA SANITIZATION AND DISPOSAL

Without ensuring the proper disposal of installed and removable digital storage, information security risks can be created by reassigning, surplussing, transferring, trading-in, disposing of computers, or replacing digital storage media and computer software. Therefore, once digital CHRI media devices are determined no longer needed by the agency, devices shall be sanitized and disposed of according to the most current FBI CJIS Security Policy. Due to the presence of temporary files (data remanence), devices where digital media was once stored, processed, and/or used for dissemination (fax, scanners, computers, laptops, etc) shall be sanitized in a manner that gives assurance that the information cannot be recovered prior to disposal of or upon the reassigning or recycling of such devices. An "erase" feature (e.g., putting a document in a “trash can” icon) or deleting a file is not sufficient for sensitive information, because the information is still be recoverable. The agency will provide steps for the sanitization and disposal of devices where CHRI media was once stored, processed, and/or used.

The Department of Licensing and Regulatory Affairs leases all computers from the Department of Technology, Management, and Budget. Part of the contract ensures the secure disposal and sanitization of all CPUs. DTMB follows the State of Michigan Technical Standard 1310.00.110.04 for the secure disposal of installed and removable digital media. The standard is found below:

State of Michigan
Technical Standard
1340.00.110.04 SECURE DISPOSAL OF INSTALLED AND REMOVABLE DIGITAL MEDIA STANDARD

Issued: 02/26/2014
Revised: 10/21/2015
Reviewed:
Next Review Date (1 yr.): 10/21/2016

Authoritative Policy: 1340.00 Information Technology Information Security Policy (http://www.michigan.gov/documents/dmb/1340_193162_7.pdf)

DISPOSAL OF PHYSICAL MEDIA
Once physical CHRI media (paper copies) is determined no longer needed by the agency, media shall be destroyed and disposed of according to the FBI CJIS Security Policy. Formal procedures for the secure disposal or destruction of physical media:

a. Large quantities of CHRI Physical Media shall be destroyed by the shredding company contracted by the State of Michigan in the presence of the LARA Non-technical LASO. The records will be maintained in a designated locked bin with the only key being secured by the LASO. The bin will be stored in a locked room while not being used.

b. All other CHRI Physical Media shall be destroyed by the cross-cut shredder available to all BDVP Staff. All CHRI shall remain under lock and key until it is destroyed.

PHYSICAL PROTECTION

LARA shall document and implement a physical protection policy and procedures to ensure CHRI and information system hardware, software, and media are physically protected through access control measures.

PHYSICALLY SECURE LOCATION
LARA will ensure both sufficient physical and personnel security controls exist for the protection of CHRI and associated information systems. A physically secure location is a facility, an area, a room, or a group of rooms within a facility. LARA will:

a. Prominently post the perimeter of the physically secured location and keep separate from non-secure locations by physical controls.
b. Keep a current list of personnel with authorized access to the physically secure location or use a method of credentials to keep track of authorized personnel.
c. Ensure all physical areas where CHRI or information systems are stored and/or used for processing shall be controlled. Individuals requiring access to such locations will be verified before granting access. Physical access to information system distribution and transmission lines within the physically secure location will be controlled and safeguarded.
d. Position information system devices that display CHRI in such a way as to prevent unauthorized individuals from accessing and viewing CHRI.
e. Ensure methods are in place to monitor, detect and respond to information system incidents for individuals attaining physical access to secured areas.
f. Validate all visitors before admittance to the physically secure locations, and visitors will be escorted and monitored at all times.
g. Authorize and control information system-related items entering and exiting the physically secure location.

CONTROLLED AREA

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CHRI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CHRI access or storage. At a minimum:

a. Access is limited to controlled area during CHRI processing times and to authorized personnel, approved by the agency to access or view CHRI.
b. CHRI will be locked and secured to prevent unauthorized access when unattended.
c. Information system devices and documents containing CHRI will be positioned in such a way as to prevent an unauthorized individual from access or view.
d. Encryption requirements will be implemented for digital storage (i.e. data “at rest”) of CHRI.

AGENCY PUBLIC HEARINGS - CRIMINAL HISTORY RECORD INFORMATION DISCLOSURE

CHRI must not be disseminated to the general public. CHRI may only be disseminated to authorized entities or individuals, whether physically or verbally. Information is considered

CHRI if it is transferred or reproduced directly from CHRI and associated with the subject of the record. This includes information such as conviction/disposition data as well as identifiers used to index records regardless of format. Examples of formal and informal products or verbalizations include:

- Correspondence such as letters and emails.
- Documents such as forms and hand-written notes.
- Conversations either in person or by telephone.
- Data fields such as those stored in a database tables or spreadsheets.

This includes maintaining CHRI in formats that are accessible by the public or within records that are subject to release through public record requests. CHRI may be disclosed as part of the adjudication process during a hearing that is open to the public if the agency demonstrates all of the following:

- The hearing is based on a formally established requirement;
- The applicant is aware prior to the hearing that CHRI may be disclosed;
- The applicant is not prohibited from being present at the hearing; and
- CHRI is not disclosed during the hearing if the applicant withdraws from the application process.

For example, as part of regularly scheduled meeting a board or commission may find a need and be authorized to discuss CHRI as part of a regularly scheduled meeting, during which applicant appeals are discussed as a standard agenda item.

NOTE: If a hearing officer or board produces a certified record of conviction (public document) as proof of an individual's ineligibility (conviction of a listed offense, for example), then in this instance the information discussed is not considered CHRI.
Even when the specific conditions are met to allow disclosure during a public hearing, the most preferable method for introducing CHRI is to enter into a closed session which limits participation by the public at large. States and local agencies should be able to reasonably demonstrate how the prerequisite criteria are being met for audit purposes.

INCIDENT RESPONSE

LARA shall establish operational incident handling procedures for instances of an information security breach. Information security incidents are major incidents that significantly endanger the security or integrity

of CHRI. The agency will identify responsibilities for information security incidents and include how and who to report such incidents to. The agency will ensure appropriate security incident capabilities exist, and should incorporate the lessons learned from ongoing incident handling activities. The agency will ensure procedures exist and are implemented for a follow-up action of a security breach and for the collection of evidence in cases of legal action. All individuals with direct or indirect access to CHRI shall be trained on how to handle an information security incident, and such training is to be included within the agency's Security Awareness Training. (See section on Security Awareness Training at the end of this document.)

Procedures shall be in place to track and document information security incidents, whether physical or digital, on an ongoing basis. When an incident has been determined a breach having to do with CHRI, the agency will report the security breach to the MSP ISO through the use of a "Information Security Officer (ISO) Computer Security Incident Response Capability Reporting," form (CJIS-016).
Department of Licensing and Regulatory Affairs Information Privacy and Security Incident Response *(G-21)*

Reference Documents
LARA Information Privacy and Security Policy *(G17)*
LARA Information Privacy and Security Handling Policy *(G-20)*
Information Privacy and Security Breach Notification *(G-18)*

MOBILE DEVICE INCIDENT RESPONSE
LARA does not allow the use of mobile devices for any CHRI purposes.

SECONDARY DISSEMINATION

When permitted by law, and LARA releases a CHRI response to another authorized recipient pursuant to authorized sharing provisions, a log of such release(s) shall be established, implemented, and kept current. The log will be maintained indefinitely and be made available upon request to a MSP representative for audit purposes. Fields required for the log are:

- The date the record was shared.
- Record disseminated.
- Requesting agency (whom the response was shared with) / Recipient Name.
- Method of sharing; either by U.S. Mail or landline fax. (No emailing).
- Agency personnel that shared the CHRI.

SECURITY AWARENESS TRAINING

LARA will establish, implement, and administer basic Security Awareness Training (SAT) that meets the minimum standards provided within the most current version of the FBI CJIS Security Policy. The LASO will, every two years and starting from date of adopting agency SAT, review the FBI CJIS Security Policy to ensure agency implemented SAT meets the most current requirement(s). All individuals having access to CHRI, whether digital or physical, shall complete SAT provided by the agency within six (6) months of assignment and every two (2) years thereafter. The agency will also include any or all Information Technology (IT) personnel having access to digital systems used to process CHRI. The agency will document and keep current completed SAT records, past and current.